**STATEMENT OF**
**JACQUELYN L. WILLIAMS-BRIDGERS**
**INSPECTOR GENERAL OF THE**
**DEPARTMENT OF STATE,**
**ARMS CONTROL AND DISARMAMENT AGENCY, AND**
**UNITED STATES INFORMATION AGENCY, INCLUDING**
**THE BROADCASTING BOARD OF GOVERNORS**

# THE YEAR 2000 COMPUTER PROBLEM: GLOBAL READINESS

**BEFORE THE**

**SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM**

**UNITED STATES SENATE**

**March 5, 1999**

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify before your committee on the international implications of the Year 2000 (Y2K) computer problem. The Y2K problem is one of the most challenging project management and systems conversion efforts ever faced by the world community. As you know, the Department's challenge in addressing Y2K extends well beyond its Washington headquarters, because failure of systems in countries hosting U.S. Government organizations has the potential to disrupt this country's ability to carry out our foreign affairs agenda and protect U.S. interests abroad in the year 2000.

## SUMMARY

My office has been actively engaged with the Department of State and our embassies overseas to assist them in meeting the Y2K challenge. Of particular interest to your Committee, my office is also assessing the Y2K readiness of host countries where the United States maintains a diplomatic presence. Our work to date assessing host country readiness has revealed some key themes:

- Industrialized countries are well ahead of the developing world; however, some of those locations are at risk of having Y2K-related failures because they were late in establishing Y2K leadership at the national level, and because they are heavily reliant on computer technology in key sectors;

- Developing countries generally are lagging behind and are struggling to find the financial and technical resources needed to resolve their Y2K problems; still, the relatively low level of computerization in key sectors (utilities, telecommunications, and transportation) may reduce the risk of prolonged infrastructure failures;

- Former Eastern bloc countries are late in getting started and are generally unable to provide detailed information on their Y2K remediation programs;

- Problems related to Y2K readiness in the health care sector are apparent in the majority of countries evaluated; and,

- An effective Y2K policy framework is needed to ensure that U.S. strategic interests are not adversely affected by Y2K-related failures on January 1, 2000.

This statement will address OIG's oversight of Y2K remediation efforts by countries that host our embassies and consulates and by the U.S. Department of State.

## BACKGROUND

On January 1, 2000, many computer systems may malfunction or produce inaccurate information simply because the date has changed. Unless prevented, these failures will adversely affect organizations and individuals around the world. Failure of host countries to resolve the Y2K problem or to create adequate contingency plans could create havoc in the foreign affairs community by disrupting messaging systems, hindering visa and passport processing at embassies and consulates, and shutting down administrative functions such as payroll and personnel actions processing.

The Department's global presence at more than 260 locations worldwide increases its challenge to continue functioning effectively in the year 2000. The Department's posts, U.S. businesses, and millions of Americans living, working, and traveling abroad rely on their respective host countries' infrastructures to provide essential power, water, and telecommunications services. In many countries, these services could be disrupted if critical components and control systems of their infrastructure are not made Y2K compliant.

Efforts to solve Y2K problems generally should follow a phased methodology with each phase representing a major Y2K segment, as described below.

- Awareness — Define the Y2K problem, obtain executive support for a Y2K program, establish a program team, and develop an overall Y2K strategy. Ensure that everyone in the organization is fully aware of the issue.
- Assessment — Assess the potential impact of Y2K on the enterprise. Inventory and analyze systems supporting core business areas and processes and establish priorities and contingency plans for their conversion or replacement. Secure the resources needed for renovation, validation, and implementation.
- Renovation — Convert, replace, or eliminate systems or components that are not Y2K compliant. Modify interfaces as necessary.
- Validation — Test and verify the performance, functionality, and integration of converted or replaced systems or components in operational environments.
- Implementation — Put the validated systems or components into production. Implement necessary contingency plans.

Under to this methodology, the assessment phase should have been completed by mid-1997 to allow sufficient time for renovation, validation and implementation. According to information technology experts, testing, which is part of the validation phase, will account for around 50 percent of the time needed to correct a Y2K problem.

Much of the Y2K readiness information obtained by both OIG and embassy staff during meetings with host country officials was provided with the understanding that it would be held in strict confidence. Consequently, this statement does not identify specific countries, except where such information has previously been discussed in the press or obtained from open sources.

## State Department International Y2K Efforts

The State Department has recognized that the potential for Y2K vulnerability is not restricted to its domestic operations and has implemented measures to assess the Y2K readiness of all countries where the United States has a diplomatic presence. In November 1998, the Department sent a cable to all of its embassies instructing them to complete a Y2K survey of their respective host country's Y2K efforts. With this survey, the posts were expected to collect information on a wide array of subjects, including the effectiveness of the countries' Y2K program, vulnerability to short-term economic and social turmoil, reliance on technology in key infrastructure sectors, and the status of Y2K correctional activities.

As of February 18, 1999, the Department had received responses from posts in 132 countries. The information from this survey, and from other sources, such as the World Bank, the United States Information Agency (USIA), and this office, is being analyzed by staff under the direction of the National Intelligence Council (NIC). The NIC is providing its analysis to staff in the State Department's Intelligence and Research Bureau. Based on these analyses the Department will determine whether it needs to issue travel warnings concerning particular countries or develop drawdown or evacuation plans for areas where the Y2K problem may pose a risk to Americans living abroad.

Toward that end, on January 29, 1999, the Department issued a worldwide public announcement on the Y2K problem to inform U.S. citizens of the potential for problems throughout the world because of the millennium "bug." The notice cited specific areas of concern, including transportation systems, financial institutions, and medical care, as activities that may be disrupted by Y2K-related failures. This announcement further warns that all U.S. citizens planning to be abroad in late 1999 or early 2000 should be aware of the potential for problems and stay informed about Y2K preparedness in the locations where they will be traveling.

## OIG Year 2000 Oversight Efforts

### International Y2K Efforts: Host Country Preparedness

OIG has been active in international Y2K issues through our efforts to establish venues for information sharing and cooperation, as well as through work performed by OIG staff to collect information on the Y2K readiness of countries where the U.S. Government maintains a presence. We analyzed Y2K host country assessments submitted over the past two months by U.S. embassies in 74 countries: 42 in the developing world, 11 from developing/former Eastern bloc, and 21 from industrialized countries. In addition, since September 1998, OIG has conducted an aggressive effort to collect and analyze information on Y2K efforts in 20 of the countries cited above. See Appendix I for a complete list of the 74 countries assessed for this statement.

In addition to consulting with embassy personnel, OIG met with host country Y2K program managers; representatives from key infrastructure sectors, such as utilities, telecommunications, and transportation; and private sector officials to discuss their respective Y2K programs and to share information. A summary of OIG international Y2K site visits is provided in Table 1. The information we collected about host country readiness provides general insight into a host country's efforts to reduce the impact that Y2K-related failures might have. However, we caution that this information represents the situation at a particular point in time. OIG visits began 5 months ago, and the situation in some of those locations may have changed. Generally, embassies' host country Y2K assessments were completed from December 1998 through January 1999.

**Table 1: Summary of OIG International Y2K Site Assessments**

| Date of Visit | Locations Visited |
|---|---|
| September 1998 | Mexico City & Monterrey, Mexico<br>Santiago, Chile<br>Panama City, Panama |
| October 1998 | Pretoria & Cape Town, South Africa<br>Libreville, Gabon<br>Yaounde, Cameroon<br>Addis Ababa, Ethiopia |
| October/November 1998 | Hong Kong<br>Bangkok, Thailand<br>Singapore<br>Manila, Philippines |
| December 1998 | Mumbai & New Delhi, India |
| January 1999 | London, United Kingdom<br>Moscow, Russia<br>Kiev, Ukraine<br>Warsaw, Poland<br>Paris, France<br>Rome, Italy<br>Athens, Greece<br>Frankfurt, Bonn, & Berlin, Germany |

OIG has provided information summaries on each of these countries to appropriate State Department staff, the President's Year 2000 Conversion Council, USIA, Congressional committees, and to other foreign affairs organizations. Generally, the information we've collected about specific countries is considered to be sensitive, with disclosure of such information intended to be made only to other governments, international organizations, and other entities which the Department determines may benefit in connection with their own Y2K activities.

OIG is also engaged in other international Y2K efforts. In accordance with a Memorandum of Understanding signed by the Secretary of State and Chile's Minister of Foreign Affairs, OIG has begun a cooperative effort to work with the Chilean Government on a number of internal audit issues. In September 1998, OIG auditors met with Chilean Government representatives to exchange ideas on addressing and enhancing Y2K-related audit methodologies.

Also, in coordination with the Organization of American States (OAS) and USIA, OIG has initiated a series of USIA Worldnet Interactives with Latin America and Canada to provide a high-technology forum for information sharing on timely contingency planning and Y2K compliance in the sectors of energy and financial institutions. In coordination with OAS and USIA, these interactive programs have been broadcast live throughout this hemisphere and worldwide via the Internet. The programs have explored problems, strategies, and solutions in Y2K readiness and have been widely viewed and well received.

**Results of OIG International Assessments**

Based on our work in the countries cited above and on our assessment of other information provided by the State Department, a number of themes have emerged relating to the potential impact the Y2K problem may have in the global arena. We are basing our assessment of host country efforts to solve Y2K problems on the countries' compliance with the phased approach discussed earlier. The phases include **awareness** of the problem at the highest levels, **assessment** of the impact of the Y2K problem, **renovation/replacement** of noncompliant systems, **validation** of renovated/replaced systems, and finally, **implementation** of the revised system.

It is critical to note that, in terms of measuring the timeliness of different Y2K stages, the **assessment** phase should have been completed by mid-1997 to allow sufficient time for renovation, validation and implementation. In conducting our analysis we combined the renovation and validation phases because they overlap; that is, system validation will often start well before the entire system has been renovated. As discussed below, many countries, especially in the developing world, remain in the assessment phase for Y2K and face increasing risk from Y2K-related failures on January 1, 2000.

Because of the sensitive nature of the information collected, this statement does not identify specific countries, except where such information has previously been

discussed in the press or other public venues. Our work has resulted in the following findings:

Inconsistent Progress in Industrialized Countries

Most of the 21 industrialized countries we evaluated (7 of which we visited) were making good progress in their Y2K remediation programs. For example, as Table 2 shows, only 5 countries were still in the assessment phase for the electricity sector, and just a scattered few remained in the assessment phase in the other critical sectors. However, a few countries were not consistently focused or effective in their Y2K efforts. Governments in several countries, for example, had started Y2K programs in mid-1998, but some of those programs were making only minimal progress. Because countries in the industrial world are highly dependent on computer technology in every sector, the potential impact of Y2K-related failures is much higher in these countries than in the developing world. Some examples of problems found in our evaluation of industrialized countries' Y2K programs are as follows:

- In one European country, the government did not recognize the serious nature of the Y2K problem and had yet to establish a formal Y2K budget. In addition, government officials in this country were not willing to provide detailed information on their Y2K efforts.
- In another European country, which expects a huge influx of tourists for millennium-related celebrations, the government had established a Y2K committee in August 1998 but did not hold the first meeting on Y2K until January 1999.
- In yet another European country, the Y2K issue was viewed as a technical problem by the government and was given low priority. Public apathy was widespread and no government leaders were willing to take up the issue.
- According to embassy reports, a number of middle eastern countries are at risk—not only because of possible disruptions in the oil industry—but because of possible Y2K problems in their desalinization plants. These countries receive most of their fresh water from desalinization plants, and would face grave survival problems if the plants lost power or encountered significant Y2K failures in their own systems.

Table 2: Y2K Status in Key Sectors in Industrialized Countries

| Y2K Phase/Sector | Electricity | Banking | Telecommunications | Air Travel |
|---|---|---|---|---|
| Assessment | 5 | 1 | 2 | 1 |
| Renovation/Validation | 12 | 15 | 13 | 17 |
| Implementation | 4 | 5 | 6 | 3 |

See Chart 1 in appendix II for a visual depiction of Y2K status in key sectors in 21 industrialized countries.

Many Developing Countries Lack Adequate Resources

Developing countries were struggling to make headway in solving their Y2K problems. These countries were generally in the assessment phase toward the end of 1998, as they endeavored to develop effective remediation plans and to address the difficult task of finding adequate financial and technical resources to resolve Y2K issues or to develop contingency plans. The governments of some developing countries did not regard Y2K as a priority and thus had not established committees or task forces to address Y2K on a national basis. In these locations, the risk of failure in such key sectors as utilities and telecommunications will depend on the extent to which these sectors rely on computers and embedded devices. In addition, these countries are generally experienced in dealing with short-term power and telecommunications outages. The question remains, however, as to how well they can handle long-term disruptions in numerous sectors that may concurrently occur because of Y2K-related failures. Examples of some specific problems facing developing countries are as follows:

- A country in Africa established a Y2K committee in September 1998, to conduct an overall assessment and increase public awareness, but allocated only $126,000 for its Y2K budget. A local newspaper headline read "**One Benefit of Being a Backward Country: No Y2K Disaster Expected** (here)", which oversimplifies the issue. In fact, in this country, critical services such as power, telecommunications, and aviation are at risk.
- Officials in another African country told us that their power generation system was Y2K compliant; however, they noted that the automated systems used by the municipalities for power distribution and billing were not compliant, and that there was little money available to fix them. The power company has threatened to cut off power to those municipalities whose distribution and billing systems have not been fixed.
- In one African country, where one-third of the workforce was employed by the government, as of January 1999 there was still no Y2K committee or point person to marshall government efforts. There were increasing concerns that social unrest could occur should the government be unable to pay government workers. In an effort to persuade the government to focus attention on the Y2K problem, the U.S. Ambassador there met with the country's President to explain the Y2K problem.

- One Asian country we visited in late 1998 was just beginning a national Y2K program at the governmental level. Government officials told us that, although their country possessed significant software development expertise, this talent was largely being used for off-shore Y2K projects. They lamented that they could not afford the Y2K services of software companies in their own country.
- Officials in another Asian country told us they'd gotten off to such a late start last year that they'd decided to go directly into contingency planning. These same officials informed us that efforts to remediate air traffic control systems were not progressing well and that they were developing plans to shut down the country's main airport on December 31, 1999, should the situation warrant such a move.
- Both the Panama and Suez Canals face the risk of disrupted operations should their traffic management systems fail, or should ships traversing either canal have problems with their engines and/or steering systems because of Y2K. Panama Canal officials told us they will not allow any ships into the Canal's locks on December 31, 1999; they further asserted that, while they were making progress toward fixing their automated ship traffic management system, they can revert to manual traffic management operations should it be necessary. According to Suez Canal officials, their traffic management system is not Y2K ready; however, the vendor, a Norwegian firm, is working on the system, and plans to have it fixed by August 1999.

Table 3: Y2K Status in Key Sectors in 42 Developing Countries

| Y2K Phase/Sector | Electricity | Banking | Telecommunications | Air Travel |
|---|---|---|---|---|
| Assessment | 23 | 9 | 20 | 19 |
| Renovation/Validation | 14 | 27 | 14 | 19 |
| Implementation | 5 | 6 | 8 | 4 |

See Chart 2 in appendix II for a visual depiction of Y2K status in key sectors in 42 developing countries.

## Difficulty in Assessing Eastern Bloc Progress

Developing countries that were part of the "Eastern bloc" (including countries that were part of the former Soviet Union) were also late in getting started and generally were still in the assessment phase at the end of 1998. Nearly all of the Eastern bloc countries evaluated are at least partially dependent on computers for such key sectors as finance, telecommunications, utilities, and transportation. Further, because the governments of these countries had not completed their Y2K assessments, we found it difficult to obtain detailed information about the Y2K programs in these countries, thus hindering our ability to analyze the progress being made. Still, we were able to obtain some key

information concerning telecommunications in Russia and power generation in both Russia and Ukraine. Specifically,

- Information technology experts in Russia told us they believe the telecommunications sector there is a major risk. Specifically, they told us that most of the local telephone exchanges use non-Y2K-compliant switches that were made in a former Soviet factory that is now defunct. Without replacement with Y2K-compliant switches, there likely will be disruptions in local telecommunications capabilities.
- During our visit to Russia, officials told us that the safety systems used in their nuclear power plants were based on analog electronic components and thus were not susceptible to the Y2K problem. They stated that other management information systems used by the plants might be affected, but they were still running tests; still, they indicated that these systems were not essential to continued plant operations. These officials were not sure whether there were any embedded devices in the nuclear power plants that would affect operations.
- According to embassy reports and our discussions with the Ministry of Energy and other experts, Ukraine's power sector may be at serious risk as a result of Y2K. Ukraine's power grid is currently fragile due to, among other things, a lack of funds to purchase much needed and expensive fossil fuel to power old and inefficient thermal heat and electricity plants. One weakness in the power grid is obsolete hardware and software systems: only two of the eight electricity management computer systems are Y2K compliant. Further, the Government of Ukraine does not at this point seem prepared to handle a long-term power outage during the middle of winter, if the electricity grid collapses.

In addition, assessing the Y2K progress of Eastern bloc countries is difficult because of apparent widespread use of pirated software, often the result of a lack of adequate financial resources. For example, officials from the energy ministry of one country told us they used mainly pirated software applications and thus could not receive Y2K remediation services from the software manufacturers. Whereas, in other Eastern bloc countries, the governments are working with vendors to replace pirated software with licensed software. Further confusing the situation in many Eastern bloc countries is the lack of information on when and where computer equipment and software were obtained in the first place.

Table 4: Y2K Status in Key Sectors in 11 Developing/Eastern Bloc Countries

| Y2K Phase/Sector | Electricity | Banking | Telecommunications | Air Travel |
|---|---|---|---|---|
| Assessment | 10 | 6 | 6 | 7 |
| Renovation/Validation | 1 | 4 | 4 | 4 |
| Implementation | 0 | 1 | 1 | 0 |

See Chart 3 in appendix II for a visual depiction of Y2K status in key sectors in 11 developing/eastern bloc countries.

Overall Lack of Y2K Readiness in the Health Care Sector

Y2K readiness in the health care sector appeared to be at risk in nearly every location evaluated. The failure of an information system or a medical device in a clinic or a hospital can put lives at risk. For example, it is conceivable that a computer might cut off important life support systems after the date change because it assumes the maintenance interval has been exceeded by one hundred years. In most of the countries we visited, efforts to assess the impact of Y2K on hospital systems and medical devices did not get under way until mid-1998, leaving very little time to remediate and/or replace noncompliant software and devices. As Table 5 shows, the majority of 74 countries evaluated were still in the assessment phase for the health care sector.

Table 5: Y2K Status in Health Care Sector in 74 Countries

| Y2K Phase/Country Category | Industrialized | Developing | Developing/ Eastern Bloc |
|---|---|---|---|
| Assessment | 14 | 36 | 11 |
| Renovation/Validation | 6 | 4 | 0 |
| Implementation | 1 | 2 | 0 |

See Chart 4 in appendix II for a visual depiction of Y2K status in the health care sector in 74 countries.

Policy Framework for Global Y2K Efforts Not Yet Established

Over the past year, different elements of the U.S. foreign affairs community have taken the initiative to promote Y2K awareness and establish venues for information sharing and cooperation. For example,

- In August 1998, the United States Information Service sent a team of Russian officials to the United States to be briefed on U.S. Y2K efforts, obtain information on remediation strategies, and discuss issues of mutual interest.

- The United Nations sponsored a global conference on Y2K in December 1998, attracting delegates from 120 countries, including U.S. representatives from USIA and the State Department.
- In February 1999, National Year 2000 Coordinators from the United States, Canada, and Mexico met here in Washington, to discuss cross-border issues related to the transition.
- Also last month, following an OIG site visit, the U.S. Embassy in Paris reported on a proposed series of bilateral Y2K efforts with the French Government, including an exchange of Y2K experts between the two countries, initiation of discussions on Y2K health care issues, and development of policy proposals to support an international Y2K effort in Africa.
- Also in February 1999, National Year 2000 Coordinators representing over 120 countries established the International Y2K Cooperation Center, an organization of senior executives that will support regional and sectoral efforts to address the Y2K computer problem. The Center will be funded through voluntary contributions to the World Bank and supported by in-kind contributions from other nations.
- Finally, the Department of Energy recently requested funding from the Congress to assist countries having Soviet-designed reactors in addressing potential Y2K failures that could cause nuclear accidents.

Despite these efforts, it is clear that a more cohesive framework is needed for the development and implementation of U.S. policy concerning the Y2K problem. In our visits to developing countries we were repeatedly questioned about whether the United States would be making funds available to support individual countries' Y2K remediation programs and for developing contingency plans. The primary arena for funding Y2K projects has been the World Bank, which has millions of dollars in grants and loans available for developing counties. However, the World Bank itself has stated that its funding is insufficient and that the industrialized countries will need to step in with financial and/or technical assistance.

Thus far, U.S. policy on global Y2K readiness has focused mainly on supporting efforts by international organizations--such as the World Bank--that provide financial assistance to developing countries. It is now time for the foreign affairs community to broaden its approach to global Y2K readiness to include a framework for determining what actions the U.S. should consider taking to protect the national interest. The Department is moving in this direction, by establishing a Y2K policy planning group, which will be responsible for assessing the global Y2K situation and recommending any policy actions deemed vital to U.S. strategic interests. Further, the Departments of State and Defense will co-chair an Interagency Working Group to develop policy options for those countries and sectors where Y2K problems could create a humanitarian crisis, or affect the U.S. security or economic well-being. The first meeting of this interagency working group is scheduled to occur in early March.

From our standpoint, and from the standpoint of many countries that are looking for U.S. leadership on the Y2K problem, both the Y2K planning group and the

interagency working group need to move quickly in making any policy determinations of where resources should be applied. It is becoming increasingly clear that there will be Y2K-related failures in every corner of the globe, some of which could prove harmful to U.S. interests. As such, having a robust Y2K policy framework in place will facilitate efforts by the foreign affairs community to decide what actions will be necessary to prevent Y2K-related problems before December 31, 1999.

**OIG work within the Department of State**

OIG is also playing a significant role in assisting the Department to meet the millennium challenge facing its information technology infrastructure, including computer software, hardware, and embedded devices. The Department has recognized that it is vulnerable to the Y2K problem and, over the past two years, has taken steps to remediate its systems and infrastructure to prevent disruptions to its critical business processes.

The Department has established a Program Management Office, which is responsible for the overall management of the Y2K program within the Department. The office's responsibilities include tracking and reporting on the progress being made by Department bureaus in remediating systems, providing technical advice and assistance, issuing contingency planning guidance, and certifying systems for Y2K compliancy. As of March 1, 1999, the Department reported that 66 percent of its 59 mission-critical systems were Y2K compliant and had been implemented, and it expects that 90 percent will have been implemented by March 31, 1999.

OIG's first series of reviews focused on assessing internal aspects of the Department's program to ensure that its systems and devices are Y2K compliant, and highlighted a number of key Y2K issues. These included the need for better tracking of applications, greater focus on the computer networks that support Department operations, more specific attention to the vulnerabilities of the Department's overseas computer networks, and more timely issuance of critical Y2K guidance.

In addition, my office has assisted in establishing a process through which the Department can certify the Y2K compliancy of its mission-critical systems. The purpose of this process, which we understand is one of the most rigorous in the Federal Government, is to provide the Department's senior management with assurance that every feasible step has been taken to prevent Y2K-related failures on January 1, 2000. We assisted in writing the detailed guidelines that each bureau must use in developing application certification packages for submission to the Y2K Project Management Office. In addition, through an agreement with the Under Secretary of State for Management, OIG is reviewing the adequacy of all certification packages for mission-critical systems before they are provided to the Y2K certification panel. Thus far, we have evaluated and provided our comments to the Department on seven application certification packages, and two of those have been officially certified.

* * * *

In summary, Mr. Chairman, our assessments of Y2K efforts in 74 countries over the past 5 months have provided a mixed picture of international Y2K readiness. In some places, we found convincing evidence that effective programs were in place in both the public and private sectors. In other places, however, the picture was either grim with no program in place and little progress being made, or inconclusive because the information provided did not contain sufficient detail to develop a reliable assessment.

Faced with a relentless and unforgiving deadline, countries have to make difficult decisions concerning the use of scarce resources to fix a problem that has not yet occurred. As such, over the coming months, the State Department and other U.S. Government agencies will need to revisit the information and the issues presented here in order to gain a better understanding of the potential global impact of Y2K. Only a concerted and consistent effort to collect and analyze the best information available will allow the U.S. Government and its overseas partners to adequately predict and prepare for those Y2K-related failures that occur after December 31, 1999, and to take the actions needed to protect global U.S. interests.

This concludes my statement. I would be pleased to answer any questions you may have.

**APPENDIX I**

## Y2K Host Country Assessments: List of Countries

### Africa

Algeria, Cameroon, Cote d'Ivoire, Egypt, Ethiopia, Gabon, Ghana, Kenya, Madagascar, Morocco, Namibia, Senegal, South Africa, Tunisia, Zambia

### Asia/Pacific

Australia, Bahrain, Bangladesh, China, Hong Kong, India, Indonesia, Jordan, Kazakhstan, Kuwait, Lebanon, Malaysia, New Zealand, Oman, Pakistan, Philippines, Saudi Arabia, Singapore, South Korea, Thailand, Turkmenistan, Uzbekistan, Vietnam, Yemen

### Europe

Austria, Belarus, Belgium, Bulgaria, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Poland, Portugal, Romania, Russia, Serbia-Montenegro, Spain, Sweden, Turkey, Ukraine, United Kingdom

### Central/South America

Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Guatemala, Panama, Peru, Venezuela

### North America

Canada, Jamaica, Mexico

**APPENDIX II**

Chart 1: Y2K Status in Key Sectors in Industrialized Countries

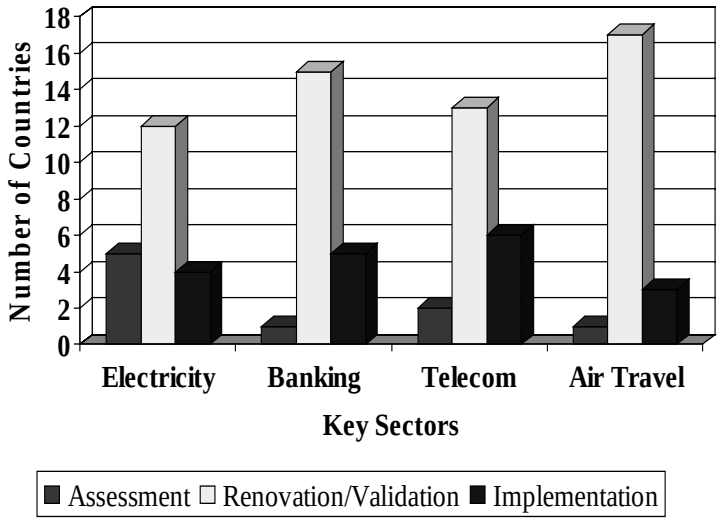
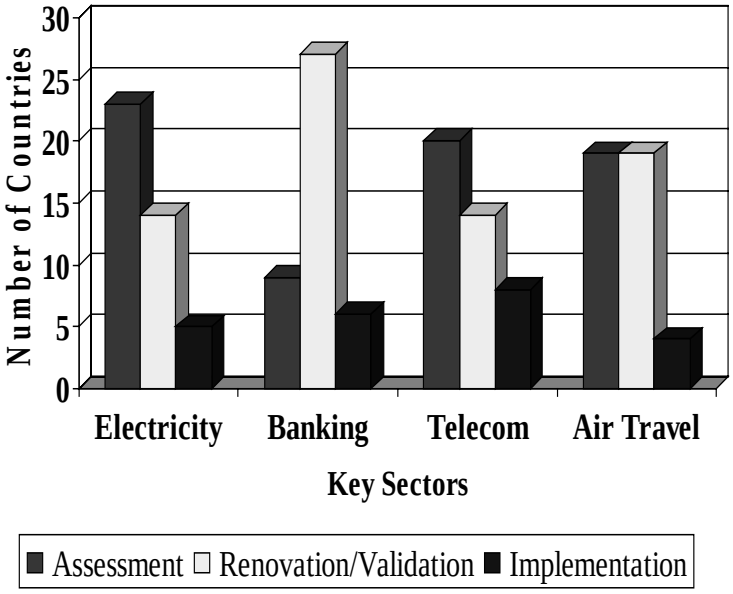



Chart 2: Y2K Status in Key Sectors in Developing Countries



**APPENDIX II**

Chart 3: Y2K Status in Key Sectors in Developing/Eastern Bloc Countries

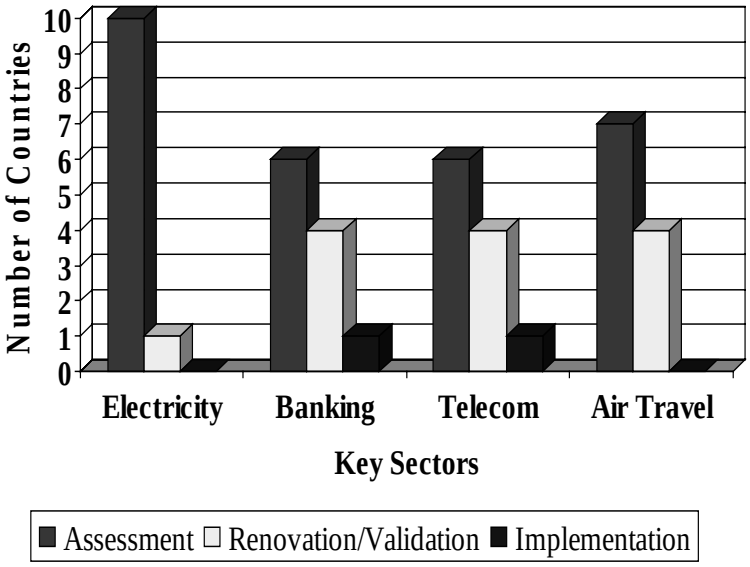



Chart 4: Y2K Status in Health Care